REMARKS

Claims 15-29, 35, 37, 38, 41 and 42 are pending in this application.

Claims 15-29 and 35, 37, 38, 41 and 42 were rejected under 35 USC §103(a) as being unpatentable over Carter (U.S. Patent No. 5,787,175) in view of Follendore, III (U.S. Patent No. 6,011,847) and further in view of Saito (U.S. Patent No. 5,740,246). The Examiner stated that the combination of Carter, as modified by Follendore, III, does not teach "a plurality of annotations generated by an annotation author, wherein access to the plurality of annotations is available to the users designated by the annotation author as having access to the plurality of annotations" and "a second multi-key encryption table comprising at least one multi-key encryption component associated with each authorized annotation user." The Examiner cited Saito for teaching these features, citing col. 12, lines 20-41 and col. 12, line 42-54 of Saito. Applicant respectfully disagrees.

Applicant's secure content object provides a means of distributing and controlling access to a document and any annotations associated with the document. The secure content object may be used in those instances when multiple authors may wish to make annotations or comments to a common electronic document and control access (and knowledge of) their annotations among other users. For example, the original electronic document may have no restrictions on viewing (all users may view it), so it is not encrypted. One or more users/authors (including the original author) may wish to make annotations or comments to the electronic document. Each annotation author may wish to limit access to one or more of the annotations. Each such annotation may be encrypted and access limited to certain users. When an authorized user inputs its user authorization information, only those portions of the document and any authorized annotations are displayed. The user sees, in the clear, only those portions of the document to which it has access.

Carter teaches a collaborative encryption method that uses structures in the prefix portion to restrict access to the information stored in the data portion. Users who are currently members of the collaborative group can readily access the information (see abstract). Follendore, III teaches a cryptographic control system for managing the encrypting keys, a key management system which keeps track of keys used with a particular message, but also maintains the

justification for the use of that key and the justification for the different categories of personnel access and the criteria used for selecting the communication system (see col. 2, lines 20-26). Saito teaches a crypt key system for use in a television system, database system or electronic commercial transaction system. Saito's crypt key system enables users, for example, to access copyrighted material stored in a database system.

1. Saito teaches a basic copyright management system for the management of the use and distribution of data.

In Saito, a first user registers with the key control center in advance for using the database. At that time, the database use program is distributed. This database utilization program includes information on the first user and a program for generating a crypt key unique to the first user with a predetermined algorithm by using the information. The data is stored in the database without encryption, and when it is distributed, the data is encrypted by the first crypt key to an encrypted data. See col. 10, lines 56-65 of Saito. The first user who uses the data directly from the database requests a key for decrypting and using the encrypted data to the key control center via the communications network. Information concerning the first user is presented at this time. See col. 11, lines 7-10 of Saito. An encrypted copyright management program (which is encrypted using a second key) is sent with the encrypted data to the user; the copyright management program describes the user's rights in the data. The first user generates a crypt key unique to the first user by using a database utilization program which is distributed in advance and using information on the first user with a predetermined algorithm. Then, the first user decrypts the encrypted copyright management program, the encrypted first and second crypt keys, and the encrypted data is decrypted by the decrypted first crypt key. See col. 11, lines 31-37 of Saito.

In Saito, the first user can transfer the encrypted data to a second user. The second user who has received the copied or transferred encrypted data requests for the secondary use of the encrypted data to the copyright management center. The second user is not required to register with the center in advance. At the time of the request for data use, with the presentation of the information of the first user from which the copyright data has been copied or transferred to the copyright control center, the request is accepted. If the first user information is not presented at

this time, the request for the secondary use is not accepted. See col. 11, line 64 to col. 12, line 9 of Saito.

2. Saito does not teach the concept of different users having access rights to only portions of document (annotations). At most Saito's copyright management system uses a different crypt key to encrypt an edited document.

Saito's copyright management system allows users to edit the data they receive, and to store and encrypt the edited data to others. In the case where new data is produced by editing a plurality of encrypted data which are obtained from the database and is encrypted to be supplied to others, the crypt key for a plurality of data which are original materials and edit program as editing process with a digital signature are used as a use permit key. See Saito col. 12, lines 42-47. This is similar to the process for transferring data from the first user to a second user as described above. The only difference is that the crypt key for the edited material is different (it is not the second crypt key). Arguably, the reason for using a different crypt key based on the edit program with a digital signature to encrypt the edited data is so the second user knows that the original data has been edited. Any user who receives the edited data receives all of the edited data.

3. Saito does not provide any means for ensuring that the second user is an authorized user; any recipient of the data that has been encrypted by the first user can receive a decryption key from Saito's copyright management system.

Indeed, any user who receives the encrypted (with the first user's information) edited data is able to decrypt all of the edited data (not just a portion of it). Saito's copyright management system does not allow the first user to restrict access to particular second users. The only way the first user can control access to the encrypted edited data (or even original data) is to hope that the second user who receives the encrypted data will not further distribute the encrypted edited data. Saito's copyright management system does not check to see if the second user is authorized by the first user; the copyright management system only checks to see if the first user/author's information is contained in the encrypted data. If it is, Saito's system will allow the second user (whether truly authorized or not) to receive the appropriate decryption keys to decrypt the data.

In contrast, with Applicant's secure content object, the secure content object can be lost to unauthorized users, none of whom will be able to decrypt any portion of the encrypted data. Any one can receive a secure content object with encrypted data; only people who have been authorized by the annotation author as evidence by "a first multi-key encryption table for use in a multi-key encryption method associated with the electronic document, the first table comprising at least one multi-key component associated with each authorized user in the first set".

4. Regarding Claim 35, Saito does not teach "wherein, responsive to an input user authorization, combining the input user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the annotation, wherein valid decryption of the annotation indicates the correct annotation encryption key has been found; concatenating the plurality of encrypted annotations in a second electronic document; and merging the second electronic document and the encrypted electronic document into a third electronic document such that access to the encrypted electronic document is available to the first set of users and access to the encrypted annotations in the separate file is provided only to authorized users."

As noted above, Saito teaches encrypting the edited data with a new crypt key. Saito does not teach combining the original data with a first crypt key, the edited data with a second crypt key and then concatenating the two together to for a third document. Also as noted above, Saito teaches that anyone having access to the encrypted data with the first user's information can gain access to the data.

5. The combination of Carter and Follendore, III and Saito does not teach Applicant's secure content object or method of forming. None of the references cited teaches encrypting annotations associated with a document differently than encrypting the original document. None of Carter, Follendore, III or Saito teaches treating access to annotations associated with a document differently than treating the document itself. Therefore, any authorized user of a particular document in Carter, Follendore, III or Saito would have the same access rights to any annotations associated with the document. The system of Saito offers no protection to the data once the first user has distributed it and a third user receives the encrypted file.

Independent Claims 15 and 35 are believed to be allowable. Since Claims 16-29 depend from Claim 15 and Claims 37, 38, 41 and 42 depend from Claim 35, they are also believed to be allowable. Claims 15-29 and 35, 37, 38, 41 and 42 are believed to be in condition for allowance.

No additional fee is believed to be required for this amendment; however, the undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025.

Reconsideration of this application and allowance thereof are earnestly solicited. In the event the Examiner considers a personal contact advantageous to the disposition of this case, the Examiner is requested to call the undersigned Attorney for Applicant, Jeannette Walder.

Respectfully submitted,

Jeannette M. Walder
Attorney for Applicant
Registration No. 30,698
Telephone: 714-565-1700

Xerox Corporation
Santa Ana, California
Date: April 7, 2006